AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Cancelled).

2. (Previously Presented) The handset according to claim 18, wherein the operating system controls the transmission of the IMEI to a mobile telephone operator by means of a secure OTA channel.

3. (Cancelled).

4. (Previously Presented) The handset according to claim 18, wherein the secure electronic module is a UICC.

5. (Previously Presented) The handset according to claim 18, wherein the operating system controls the authentication of the secure electronic module by the storage support module.

6. (Previously Presented) The handset according to claim 5, wherein the secure electronic module and the storage support module store encryption keys that are used to encrypt the secure communication channel.

7. (Previously Presented) The handset according to claim 18, wherein the secure electronic module blocks the use of the handset when a false IMEI is detected.

8. (Cancelled).

9. (Previously Presented) The method of claim 19, wherein the secure electronic module transmits the IMEI to the mobile telephone operator over a secure OTA channel.

10. (Previously presented) The method of claim 9, wherein the operator compares the IMEI with a black list of stolen handsets, and blocks the communications of the handset when the handset appears on the black list.

11. (Previously Presented) The method of claim 19, wherein the secure electronic module blocks the use of the handset when a false IMEI is detected.

12. (Previously Presented) The handset according to claim 4, wherein the operating system controls the authentication of the secure electronic module by the storage support module.

13. (Previously Presented) The handset according to claim 4, wherein the secure electronic module blocks the use of the handset when a false IMEI is detected.

14. (Previously Presented) The handset according to claim 5, wherein the secure electronic module blocks the use of the handset when a false IMEI is detected.

15. (Previously Presented) The handset according to claim 6, wherein the secure electronic module blocks the use of the handset when a false IMEI is detected.

16. (Previously Presented) The method of claim 9, wherein the secure electronic module blocks the use of the handset when a false IMEI is detected.

17. (Previously Presented) The method of claim 10, wherein the s secure electronic module blocks the use of the handset when a false IMEI is detected.

18. (Currently Amended) A telephone handset, comprising:

a storage support module storing an International Mobile Equipment Identity (IMEI) associated with an operator of a communication network ~~and a first key~~;

a secure electronic module ~~storing a second key~~;

a processor;

a memory device including program instructions that, when executed by the processor, control the handset to:

authenticate, by the secure electronic module, the storage support module;

establish, in the event the secure electronic module determines that the storage support module is authentic, a secure communication channel between the storage support module and the secure electronic module;

~~encrypt, by the storage support module, the IMEI using the first key;~~

transmit, via the secure communication channel, the ~~encrypted~~ IMEI from the storage support module to the secure electronic module; and

~~decrypt, by the secure electronic module, the encrypted IMEI received from the storage support module using the second key;~~

enable, by the secure electronic module, the handset to access the communication network ~~in the event the secure electronic module determines that the decrypted IMEI received from the storage support module is authentic; and~~

~~access, by the handset, the communication network~~ using the ~~authenticated~~ IMEI~~, wherein the network grants access to the handset without further authentication of the authenticated IMEI~~.

19. (Currently Amended) A method of securing a telephone handset, said method comprising:

authenticating a storage support module by a secure electronic module, said storage support module storing an International Mobile Equipment Identity (IMEI) associated with the operator of a communication network;

establishing, by a processor in the event the secure electronic module determines that the storage support module is authentic, a secure communication channel between the storage support module and the secure electronic module;

~~encrypting, by the storage support module, the IMEI using a first key;~~

transmitting, via the secure communication channel, the ~~encrypted~~ IMEI from the storage support module to the secure electronic module; and

~~decrypting, by the secure electronic module, the encrypted IMEI received from the storage support module using a second key;~~

enabling, by the secure electronic module, the handset to access the communication network ~~in the event the secure electronic module determines that the decrypted IMEI received from the storage support module is authentic; and~~

~~accessing, by the handset, a communication network~~ using the ~~authenticated~~ IMEI~~, wherein the network grants access to the handset without further authentication of the authenticated IMEI~~.

20. (Currently Amended) A telephone handset, comprising:

a storage support module storing an International Mobile Equipment Identity (IMEI) associated with the operator of a communication network ~~and a first key~~;

a secure electronic module ~~storing a second key~~;

means for authenticating the storage support module by the secure electronic module;

means for establishing, in the event the means for authenticating determines that the storage support module is authentic, a secure communication channel between the storage support module and the secure electronic module;

~~means for encrypting the IMEI using the first key;~~

means for transmitting, via the secure communication channel, the IMEI from the storage support module to the secure electronic module; and

~~means for decrypting the encrypted IMEI received from the storage support module using the second key;~~

means for enabling the handset to access the communication network ~~in the event the secure electronic module determines that the decrypted IMEI received by the secure electronic module; and~~

~~means for accessing a communication network~~ using the ~~authenticated~~ IMEI~~, wherein the network grants access to the handset without further authentication of the authenticated IMEI~~.